Publication date:
May 2022
Authors:
Hollie Hennessy
Mike Sullivan-Trainor

Security Threats to Your Smart Home

Effective measures to counter threats

Brought to you by Informa Tech

Omdia commissioned research, sponsored by Callix

Contents

Executive Summary

The scale of smart home devices expands the attack surface

By 2025, nearly a quarter of the world's over-two billion households will occupy smart homes, while a third will be broadband service users. The number of connected devices for electronics, house controls, and utilities will reach nearly five billion. This figure does not include the billions of connected computers, TVs, mobile phones, and tablets. While this connected world will usher in increased convenience and automation across home ecosystems, it will also greatly expand the attack surface for cybersecurity hackers and criminals.

To counter this threat, security solution providers produce more than $27bn annually in protective goods and services, yet consumers continue to lose more than $1bn a year owing to cybercrime. Clearly, further measures must be taken to manage the threat of cybercrime facing smart homes.

The first step toward a solution is to better understand where and how attacks are deployed. This report characterizes threats at a high level and offers solutions. The threat areas examined include the following:

- Hackers entering the home network through smart thermostats, consumer electronics, lighting, and utility devices
- The limitations of currently available physical safety and security devices to address the cybersecurity environment
- The major threat of staged lateral attacks, in which a hacker breaks in through one device to gain access to a network and ultimately the home gateway or router, which opens access to other connected devices that store user identities and financial information

There is no silver bullet, but solutions are evolving

While there is no silver bullet against these threats, combining the best physical, PC, and mobile device and network security can significantly increase a smart home's level of protection. Network solutions offer a good combination of threat detection and monitoring, as well as measures to shut down devices or network segments when an attack is discovered. Network-based smart home security solutions are offered by communications service providers (CSPs) and often bundled with other services to mitigate costs.

Consumers should review their smart home network ecosystem and develop a comprehensive view of what devices are connected and how well they are protected. They should also deploy an effective network-wide solution to manage all connections from a single point of control or segment networks to isolate the most sensitive data from potential lateral attacks.

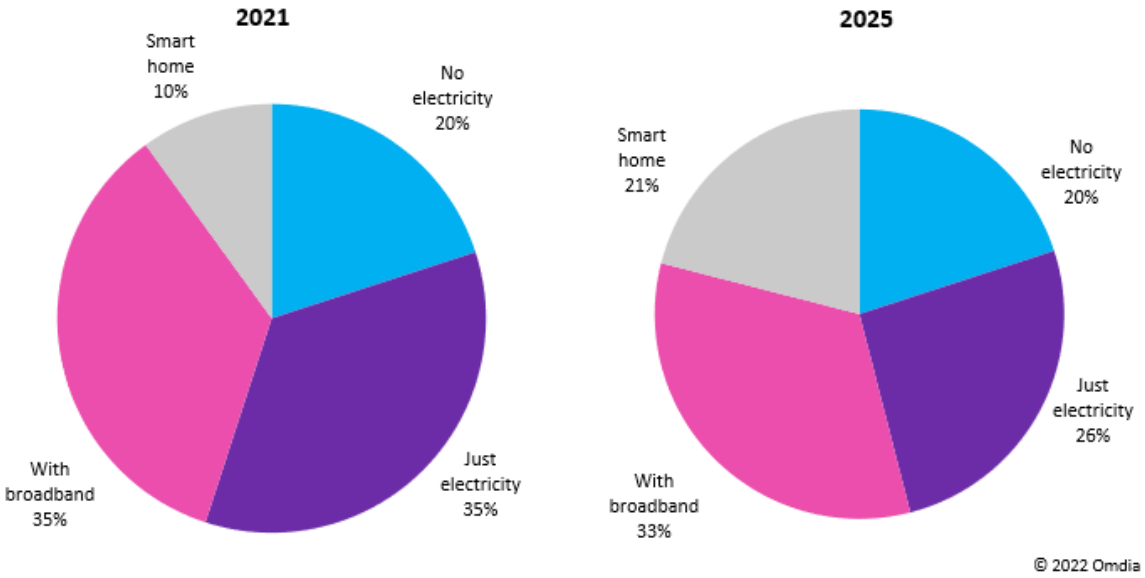
The connected smart home: A world of devices, a world of threats

What you need to know to protect your smart home from cyberattacks

By definition, your smart home is controlled by a host of connected devices—more than 10 per household, according to recent estimates. While these devices, from lighting to appliances, provide a world of convenience, they also greatly expand the cyber threat landscape. In short, the smart home is not automatically the secure home.

In fact, it can be the opposite, as millions of Peloton exercise bike users found in June 2021. It was discovered that anyone with access to the Bike+ product could corrupt the machine by installing programs, modifying files, and/or setting up remote backdoor access over the internet. Fortunately, McAfee identified the threat and fixed the issue before any individuals, gyms, or organizations were harmed—at least that we know.

Figure 1: Worldwide households (2.04 billion) by type, 2021 and 2025



Source: United Nations and Omdia

Whether we have intentionally or unintentionally made our home a smart home, each of us have multiple connected devices that we use daily such as mobile phones and laptops. However, the smart home is made of so much more—from fitness watches to thermostats that control the heating. The 2019–20 pandemic accelerated spending on these smart devices owing to the need to stay at home and communicate virtually during lockdown periods. Many of us also spent more on our homes, especially if holiday travel restrictions left us with more disposable income. We have been buying new connected devices (such as smart doorbells or even smart washing machines) to make our lives more comfortable and manageable. Yet, with each purchase and device added to the network, we can become increasingly vulnerable to cybercrime.

This report looks at the expanded threat landscape enabled by the smart home and its connected devices, many of which can be remotely compromised. Such threats extend to medical devices, including doctor-prescribed devices such as pacemakers or blood glucose monitors. The vulnerabilities of connected devices are many and widespread.

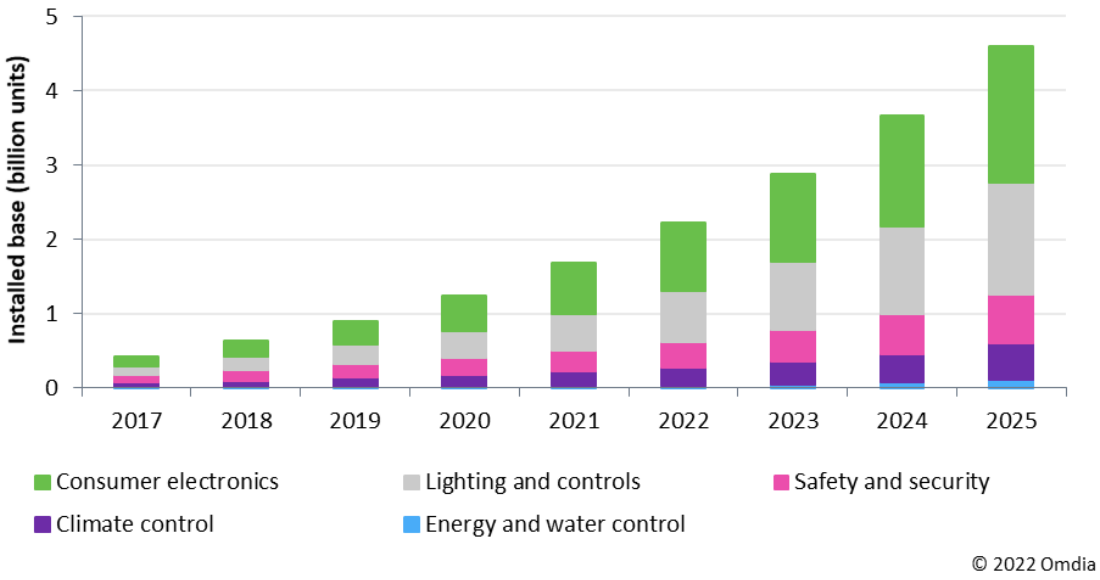
The scope of the problem – A smart device for everything

According to the United Nations, there are 2.04 billion households in the world, and according to Omdia, 21% of homes will be smart homes by 2025. This growth will be driven by smart lighting and controls and consumer electronics—the latter making up 40% of the total smart home IoT device installed base in 2021. The most popular devices in consumer electronics are smart home audio

devices, which includes products with internet access such as the Google Home and Amazon Echo. The installed base for these products has quickly grown from 72 million in 2017 to 464 million in 2021. Omdia forecasts that this figure will keep growing to reach 1.2 billion by 2025.

Smart appliances are the second most popular in the installed base; such devices include connected washing machines, clothes dryers, dishwashers, refrigerators, and large cooking appliances. Smart appliances can remotely receive, interpret, and react to signals from home automation systems, smartphones, smart TVs, or energy service providers or utilities.

Figure 2: Smart home IoT device installed base forecast by category, 2017–25



Source: Omdia

Smart health devices including sport and fitness devices, digital pill dispensers, personal scales, and digital thermometers had the smallest share (14%) of the installed base in 2021, but are increasingly popular. These devices make up the fastest-growing segment, and Omdia forecasts they will account for 17% of the installed base in 2025.

There are also smaller devices that are connected in high volumes to the network. Shipments of smart lighting and control devices, such as smart plugs, have grown from 112 million in 2017 to 497 million in 2021. Omdia forecasts they will rapidly grow to reach 1.1 billion in 2025.

With these segment categories, it is clear how a regular home can quickly become a smart home. Alongside popular personal assistant devices, adding a fitness monitor, a couple of smart bulbs and plugs in each room, and a smart washer, dryer, and dishwasher easily adds up to a total of 10 devices. This is without adding smart climate control devices (i.e., air conditioners and thermostats)

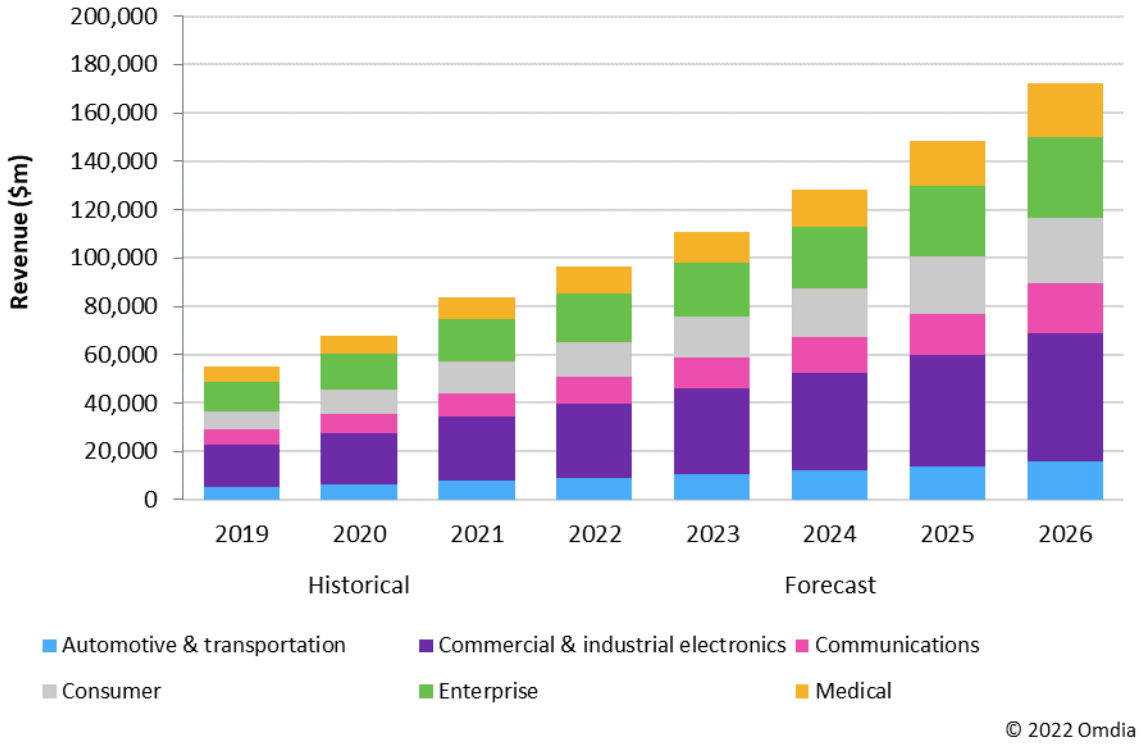
or safety and security devices (i.e., video cameras and alarms), which are forecast to reach an installed base of more than half a billion (656 million) by 2025.

Device security is far from automatic

The problem with smart devices, especially consumer devices, is that they are notoriously insecure. When adding these devices to our networks, they seem great—why not control your heating while you are out, so it is nice and warm by the time you arrive home? However, device manufacturers have not been focusing on cybersecurity. Device manufacturers tend to be more focused on a product's performance or the convenience for users (and keeping costs down to drive volume sales). In addition, white goods manufacturers are not rooted in the IT world and may not have the cybersecurity expertise that should go alongside the manufacturing and designing of connected devices. Inevitably, whether these devices are secure or not, they are added to our home networks one by one, creating entry points for cybercriminals. As we add more and more devices to a network, the cyber risks only get bigger.

What is being done to protect connected devices?

Figure 3: Global supplier revenue for connected device security by segment



Source: Omdia

There are solutions in the market to protect consumer devices. However, the area of consumer cybersecurity solutions appears somewhat neglected compared to enterprise or industrial solutions. Revenue for suppliers of consumer cybersecurity solutions for connected IoT devices currently stands at $14.6bn, or about 15% of the market, in 2022.

However, over the next few years, Omdia expects growth in the consumer segment to reach $27.5bn, or 16% of the market, as consumers become more aware and education on cybersecurity increases. In addition, governing bodies are working to better protect consumers from cybercrime through standards and regulations for products and services, such as the following:

- The UK's proposed IoT Cybersecurity legislation has been developed for consumer devices, ensuring that manufacturers define a support period at the point of sale. The legislation also bans default passwords and mandates having a point of contact for vulnerability disclosure.
- Following the US' signing of the Internet of Things Cybersecurity Improvement Act in December 2020, the National Institute of Standards and Technology (NIST) has released draft guidance setting out federal IoT cybersecurity requirements for public review. This year, the NIST is also looking to address public comments on its Cybersecurity Framework (CSF) and set forth ways to improve the framework.
- The European Commission's Cybersecurity Strategy aims to bolster cybersecurity to allow a digital and connected Europe, with the concurrent tabling of a legislative proposal for a revised NIS Directive (NIS2), modernizing and building on the existing legal framework.

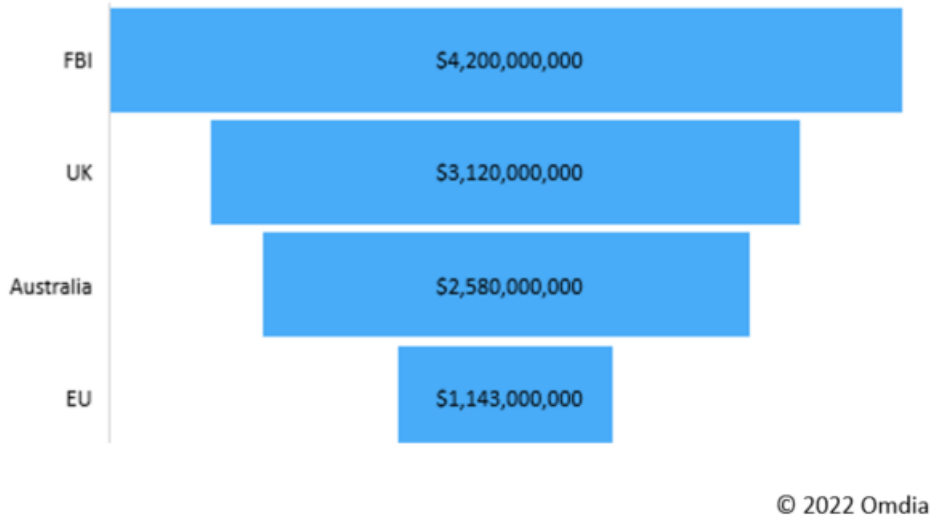
In addition, consumers are already protecting their homes with antivirus software, VPNs, content blockers, and associated products from vendors such as Kaspersky, NortonLifeLock, Avast/AVG, McAfee, Trend Micro, and more, which all provide free-to-use versions of their software. Most internet service providers (such as AT&T, Comcast, Verizon, etc.) also include security solutions with their offerings.

However, it does not stop there. Some of these companies, and others, are expanding to offer wider solutions that protect smart homes, including more functionalities allowing users to control and manage devices on their network and the security of these devices.

The cost of cybercrime

It is next to impossible to know the true costs of cybercrime for consumers because of variations in threats and a lack of consistent reporting but estimates range from $1tn (according to McAfee) to between $1–4bn.

Figure 4: Estimated costs of cybercrime for consumers



Source: Omdia

These estimates mainly cover consumer losses reported by companies that serve consumers, rather than individuals and households. In addition to these tangible losses, there are also non-monetary losses to consider such as data loss or theft, reputational damage, time to sort things out, replacing an infected kit, emotional trauma, and more. There is a wide range of potential consequences from cybercrime associated with smart home devices.

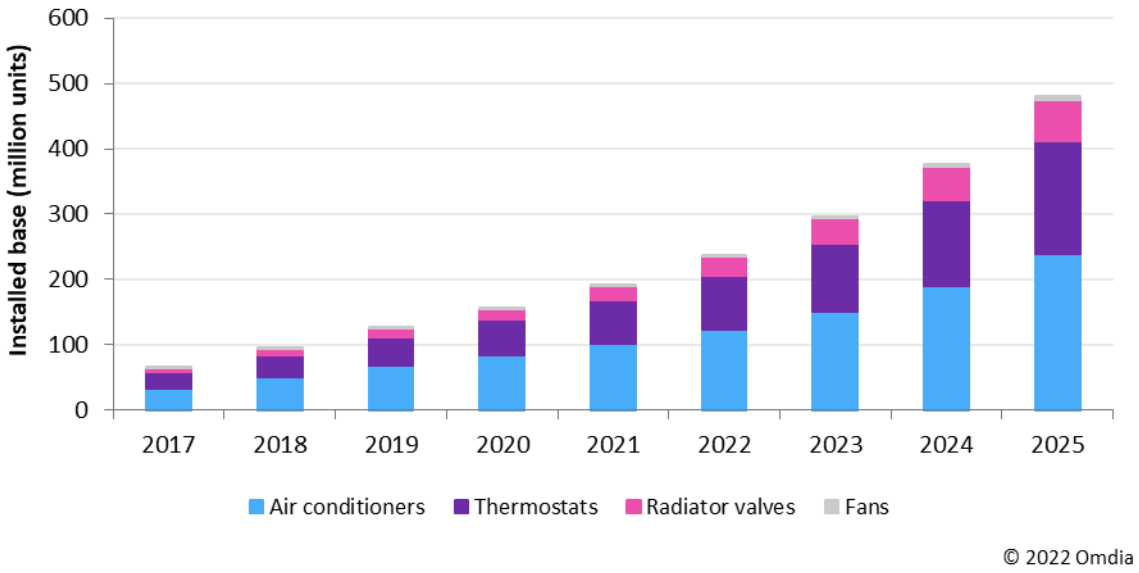
Characterizing the threats

Smart home cybersecurity threats range from attacks on individual devices and device category compromises to network assaults. To understand how to guard against such threats, gaining knowledge of attack types is the place to start.

Climate control raises the temperature

Annual shipments of climate control devices increased from 29 million units to 59 million units between 2017 and 2021. Omdia expects shipments to reach 158 million units in 2025, with smart thermostats growing faster than the other offerings. Hackers can target these devices, as demonstrated when Fox 6 reported in September 2019 that a Milwaukee couple (users of a Google Nest smart thermostat) “were left feeling ‘violated’ after their home camera began talking to them, their thermostat suspiciously topped 90 degrees, and vulgar music blasted through their wireless electronics.” While this vulnerability did not originate with the device itself—Nest confirmed that the device was not breached, but the customer had their password compromised—it shows the havoc a hacker can wreak in a smart home, how a hacker can move between devices, and how important it is to have additional security for your home. If there was additional protection—protected passwords and the ability to detect suspicious activity—the breach may not have occurred.

Figure 5: Climate control IoT device shipments unit forecast by offering, 2017–25

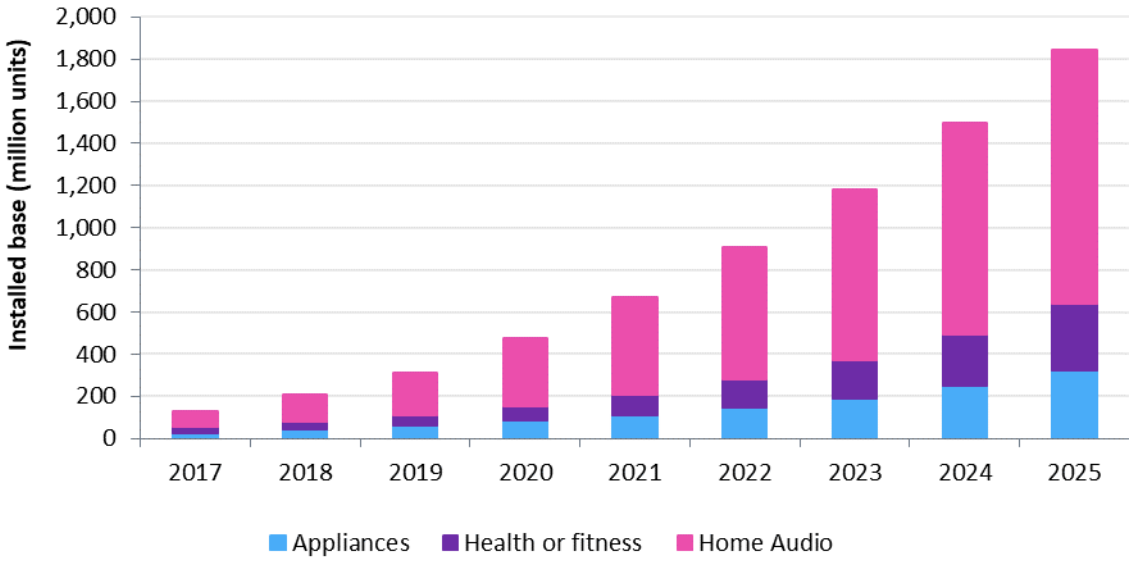


Source: Omdia

Consumer electronics eavesdropping

Shipments of consumer electronics increased from 68 million units in 2017 to 277 million units in 2021. Omdia expects shipments to reach 609 million units in 2025 with appliances and health or fitness devices outgrowing the already more established home audio devices. Over the last few years, cybersecurity companies have unearthed numerous vulnerabilities in both the Amazon Alexa and Google Home smart home audio devices that could allow criminals to eavesdrop on conversations and/or launch phishing attacks—for instance, by asking unsuspecting users to reveal their passwords.

Figure 6: Consumer electronics IoT device shipments unit forecast by offering, 2017–25



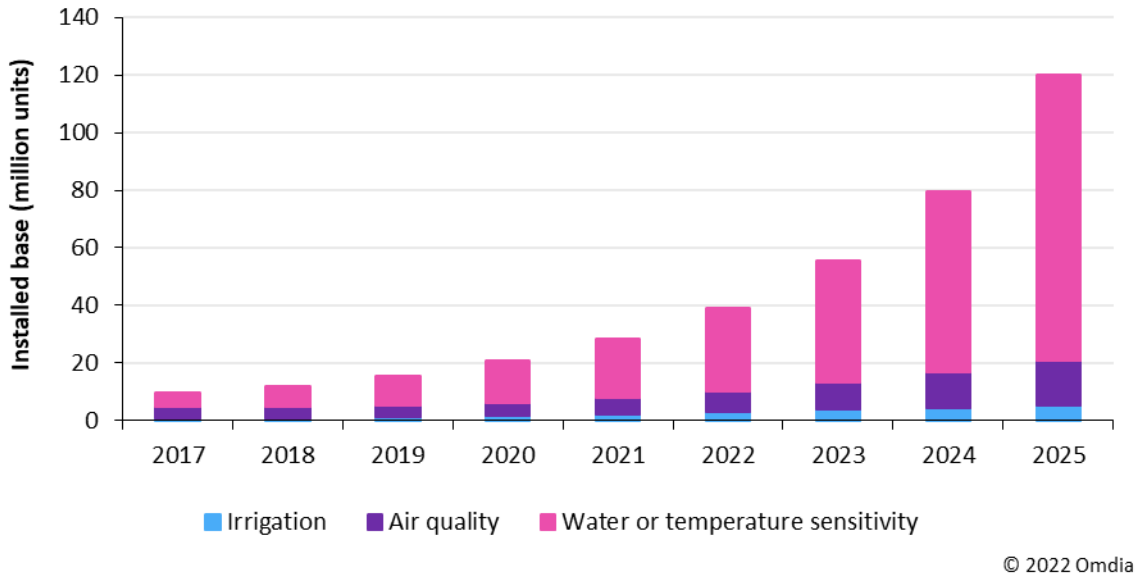
Source: Omdia

According to research from security vendor Check Point Software from June 2020, consumer electronics are vulnerable to cross-origin resource sharing (CORS) misconfigurations and cross-site scripting, which ultimately allow a hacker to perform actions on a victim's behalf—for instance, gaining access to a victim's voice history, which could reveal any of their interactions with Alexa, or gaining access to personal information from the victim's user profile. Such vulnerabilities continue to be reported, despite vendors patching their software. The vulnerability mentioned here was reported and fixed by Amazon.

Energy and water controls used for network access

Energy and water control device shipments grew from 3 million units in 2017 to 10 million units in 2021. Omdia expects shipments of these devices to reach 52 million units in 2025, with water and temperature devices becoming even more dominant within the category.

Figure 7: Energy and water IoT device shipments unit forecast by offering, 2017–25



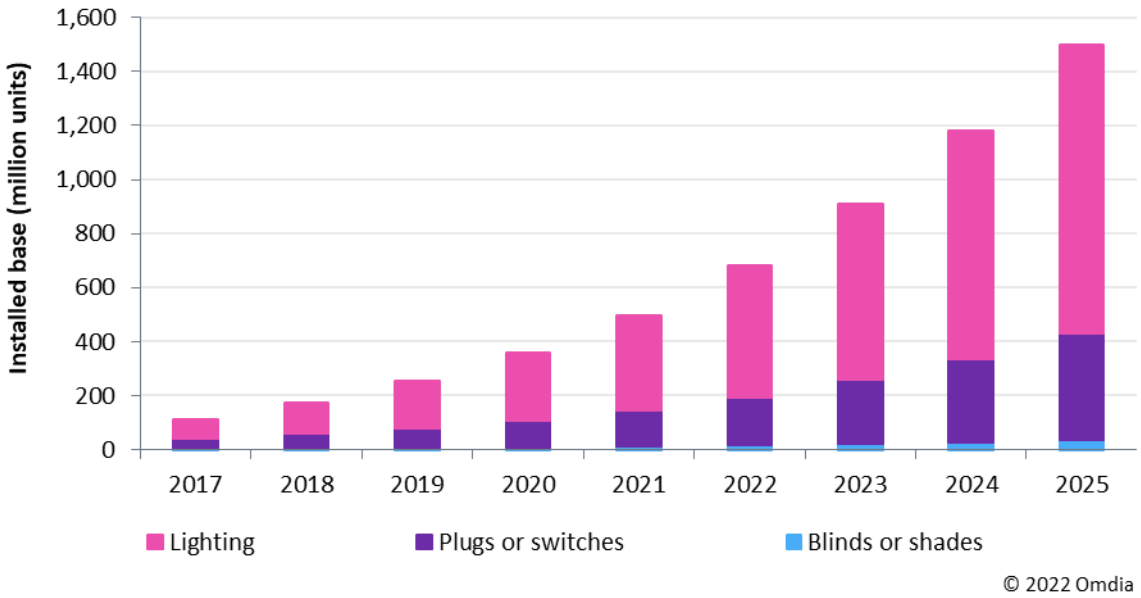
Source: Omdia

Nicole Eagan, chief strategy officer and AI officer at Darktrace, reported at a Wall Street Journal CEO Council in April 2018 that a smart thermometer in a casino's fish tank was hacked. The hackers were able to move through the network and found a database of high rollers.

Lighting and control devices provide hackers entry into other devices

Lighting and control smart devices are already being shipped in greater volumes, rising from 60 million units in 2017 to 223 million units last year. The trend is set to continue, and Omdia expects shipments to reach 600 million units by 2025. As mentioned, adding these devices to a network can rapidly add to the total number of connected devices. There are also numerous lesser-known brands of smart lighting and control devices that are attractive to consumers thanks to their low prices, but these devices show no indication of good security.

Figure 8: Lighting and control IoT device shipments unit forecast by offering, 2017–25



Source: Omdia

Researchers from UK consumer reports company Which?, in collaboration with cybersecurity consulting firm NCC Group, tested a mix of smart plugs from popular online retailers with a mix of known brands (such as TP-Link and Hive) and those less well-known. Of the 10 smart plugs tested, 13 vulnerabilities were found among 9 of the plugs. Similarly, Pen Test Partners, a cybersecurity testing firm, found they were able to hack Philips Hue bulbs owing to a lack of encryption (which Philips subsequently fixed).

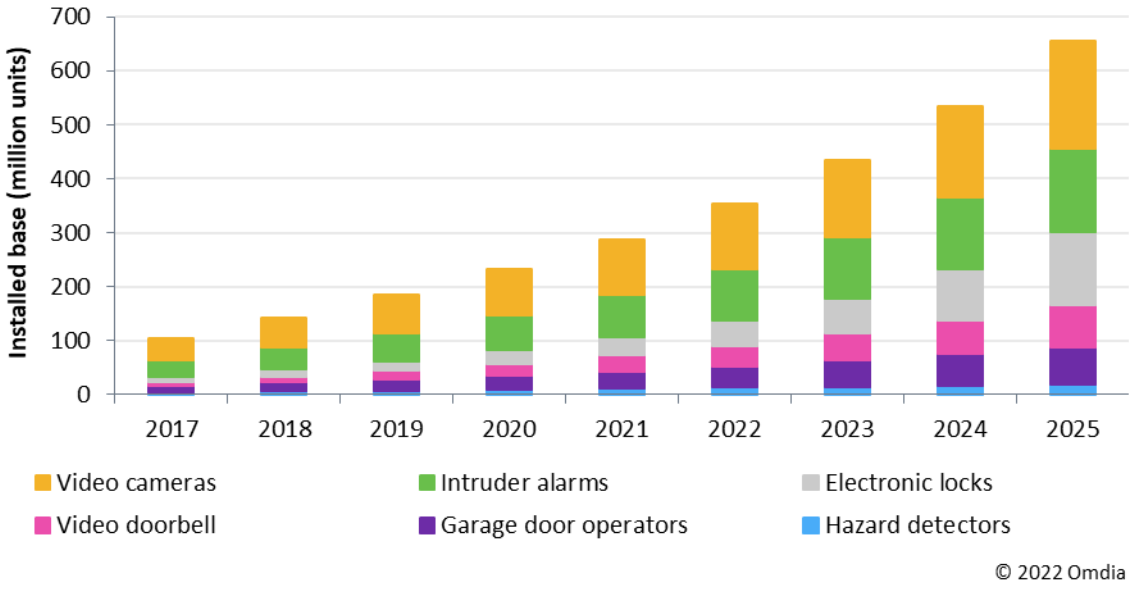
The vulnerabilities found by Pen Test Partners could allow hackers to tamper with lights—for instance, flashing lights on and off, which may seem trivial and definitely not as scary as turning the temperature up as high as possible. However, the risk is that hackers are always trying to find a "way in." Targeting devices that are known to have poor or little security could allow a hacker to enter a network and progress to more complex devices, such as home routers, or even see into users' homes with connected cameras.

Safety and security devices not secure

Shipments of safety and security smart devices more than doubled between 2017 and 2021, from 44 million units to 98 million units. Omdia expects similar growth with 224 million units forecast to be shipped in 2025. While electronic locks made up a relatively small portion of this segment in 2021, they are increasingly being implemented in homes; we expect this to be the fastest growing device. However, while used to protect our homes physically, these very devices can open the door to hackers. In November 2019, NBC reported that a Seattle couple's Taococo baby monitor had been

hacked, allowing the cybercriminal to remotely look around their home and converse with their three-year-old daughter.

Figure 9: Safety and security IoT device shipments unit forecast by offering, 2017–25



Source: Omdia

The big threat – Staged lateral attacks

As disconcerting as the vulnerabilities in individual devices are, the ultimate threat from hackers in a smart home is that of a lateral staged attack. A lateral attack is when a hacker takes over a network, device by device, positioning themself either to capture all activity for their own use, or to trawl through networks to get to the most valuable data such as a user's personal identity and financial accounts. While there are no known cases of extensive and consistent lateral attacks, there are examples of hackers using the network to access a particular piece of data; for example, the high-roller database accessed through the network from the smart thermometer in a casino's fish tank.

Lateral stacks are concerning because hacking tools such as Wireshark, Nmap, Fiddler, Metasploit, and Maltego allow anyone with knowledge of networking and Linux to invade networks and discover devices. In other words, getting into your smart home network is relatively easy for hackers. According to device intelligence security provider Senrio, an attack may look like the following:

- **Step 1:** Exploiting the camera – Using remote configuration services for commercial cameras, the hacker can open a port and access user privileges, eventually making their way to accessing executable code. The hacker then gains control by resetting the camera to factory settings, rebooting it, and preventing detection, while changing network settings.

Figure 10: Surveillance camera

Source: Omdia

- **Step 2:** Surveillance camera Detecting the router – Most smart homes have small routers or devices which provide access to the internet and interconnect all smart devices in the home. While the router prevents devices from "talking" to each other without permission, using the camera, the hacker can detect the router and its Internet Protocol (IP) address. Through the camera, the hacker can communicate with the router to gain access credentials. Using online information about router types, the hacker can compromise the routers.

Figure 11: Smart home router

Source: Omdia

- **Step 3:** From the router, the hacker can access any connected device, including personal computers where identity credentials and financial accounts are often stored.

Figure 12: Laptop

Source: Omdia

Cybercriminals like nothing more than a new challenge, and the growing proliferation of smart speakers, safety monitors, TVs, thermometers, and more is allowing them to try innovative ways to steal identity information and unprotected data.

What you can do to protect your smart home

There are three types of solutions in and around the smart home, for which security measures can be applied to safeguard against the vulnerabilities discussed and quantified above; each has its own set of suppliers, which are as follows:

- Physical security – Suppliers of connected home security systems, including smart home devices and associated monitoring services
- PC or mobile security – Antivirus software, operating systems, and Virtual Private Network (VPN) suppliers
- Network security – Internet-based service providers offering security, monitoring, analysis, and protection through broadband, cable, and telecom suppliers

While the industry has decades of experience in protecting home computing devices from virus and external cyberattacks, securing physical connected devices is relatively new, and protecting them in the home (as opposed to in the business or factory) even more so.

As a user, you can take some security measures yourself, such as:

- Changing default passwords for routers and other hardware
- Securely setting up the local area network in line with operating system suppliers' recommendations

Beyond that, almost all connected devices in a smart home require protection from suppliers via the internet itself. For example, most water, electricity, gas, and other appliances are increasingly added as nodes on the home network.

Physical security suppliers – Proprietary devices, limited network control

The first external vendors to provide home security were the physical suppliers of CCTV cameras, gates, locks, intruder alarms, and similar devices. Examples include ADT, Ring, and Vivint. Their services were based on employing people to install and maintain customer equipment, occasionally monitor the equipment, and react to break-ins and vandalism. These vendors' products and approaches have typically been proprietary and sometimes closed even to their customers; this means you may have to call them in to replace backup batteries in an alarm.

The type of security devices sold by these vendors is being digitized, which expands the scope and depth of services they can run. As defenders of the smart home, they have some advantages, which are as follows:

- Security is their business, so they are more likely than their manufacturers to see and understand the vulnerabilities associated with these new devices.
- They typically employ staff to monitor, react, and rectify potential and/or successful criminal intrusions.
- At least for cameras, locks, and alarms provided to home customers, these vendors arguably understand their roles as security providers and device vulnerabilities better than other types of security vendors.

Figure 13: Physical security suppliers

Source: Omdia

However, the nature of their business is also a cause for weakness in the face of dynamic growth in non-security-focused smart home devices, for the following reasons:

- As proprietary suppliers, these vendors' solutions may limit the selection of devices available to a customer. Many of these vendors have possibly not even considered the security implications of smart audio or smart appliances on the overall security of the home.

- As an employer of installers and monitoring systems, the costs of their systems and services tend to be higher, and they are arguably less likely to use AI software to help with security.
- Many of these vendors have not yet crossed over from providing security against physical intruders to address cybercrime.

These companies tend to identify and fix vulnerabilities in new devices they install as part of their services to consumers. However, they will likely become less relevant as more of our home experiences are virtualized.

PC or mobile suppliers – Gaps in device coverage

Numerous software companies have been protecting home computers ever since the PC market saw development, alongside advancements in hacking. These companies were eventually joined by Microsoft, which added its own free-to-use Defender antivirus software in 2006 after many years of leaving it to third parties. The primary focus for these vendors is on protecting computers, tablets, and (sometimes) smartphones used by consumers, rather than the home networks on which they run.

Figure 14: PC or mobile suppliers

Source: Omdia

Today, the strongest antivirus suppliers are Avast/AVG, McAfee, Norton, and Trend Micro. They have widened the vulnerabilities covered by their products to include Apple iOS-based client devices, VPNs (which use borrowed IP addresses to hide the identity of their users), parental controls, cloud protection, directory cleaners, password managers, and occasionally IoT device and automotive coverage.

As potential protectors of smart homes, they have numerous advantages over the other two types of suppliers covered in this section, which are as follows:

- These vendors already cover hundreds of millions of home computers, tablets, and smartphones through free-to-use offerings and tens of millions with paid subscriptions. Many consumers assume that they will be able and willing to cover IoT devices as well.

- Through continuous experiences with their users, these vendors have developed a better knowledge of cybercrime and criminal activities than many other suppliers; they discuss new vulnerabilities and fixes in blog posts and the media.

- These vendors have many years of experience protecting and helping customers recover from cyberattacks. They understand the scale and costs of attacks better than most.

Despite these clear advantages, antivirus vendors also have weaknesses when it comes to extending their protection across the smart home, which are as follows:

- These companies all offer large discounts on first-year subscriptions, forcing their customers to pay more than double for the (compulsory) second year. This business model often disappoints many of their subscribers.

- The protection they provide is for (and installed on) IT devices purchased for the home. Not only are many home users unaware that some of their newly bought IoT devices are connected or hackable by cybercriminals; they are also unaware that every antivirus supplier has gaps in their coverage of these devices.

- The natural relationships between antivirus companies and their B2B partners have dwindled over the years. Few PC manufacturers include free subscriptions to antivirus software installed on new computers, while even fewer CSPs include free or discounted subscriptions.

Many cyberattacks on the smart home will access home IT systems by exploiting poor passwords on routers and IoT devices and using Linux and machine code; although connected, these devices are often considered beyond the scope and technical capability of these antivirus solutions.

Network suppliers – Vendor-neutral network control, device gaps

Most broadband services to the home are delivered by CSPs, including wireless and wired telcos, subscription TV vendors, and others. They have numerous legal responsibilities to protect their users' privacy and security. They also buy cloud and other services, including network monitoring, management, and analysis, from other network suppliers to extend the quality of services they provide.

Network suppliers that can help by working with CSPs include Allot Communications, Bitdefender, Calix, Cujo AI, and F-Secure. The CSPs they work with include AT&T, Comcast, and Verizon. The strengths and weaknesses of these solutions for the smart home are as follows:

- Extending network security to consumers to cover smart home devices, allowing consumers to protect some (but probably not all) devices, respective of the hardware or service vendor

- CSPs can provide consumers with smart home security offers bundled with other services, which can be more cost-effective and simplifies consumer purchasing

Figure 15: Network suppliers

Source: Omdia

However, new devices may not be covered by these services if the devices communicate or operate in unexpected ways, especially devices from physical security suppliers. Some devices, such as those from utility providers, do not use home broadband connection for communication. However, network security solutions do detect intrusions and can disable a connected device. This capability may be the best way to head off a staged lateral attack.

Conclusion: Proactive steps to mitigate threats

In the race between smart home protection and cybersecurity threats, it often feels like threats are multiplying faster than we can solve them. However, consumers can take proactive steps by assuming control of their own networks and devices. For now, this means employing a combination of solutions rather than a single silver bullet.

First, install the latest security software for your PCs and mobile devices. Then, inventory all connected devices and upgrade them to have the latest security features from each supplier. Since most threats come from hackers traversing the network, consumers can limit the damage by working with network providers and their security solutions to close any gaps in network coverage, by doing the following:

- Change router and switch default settings to make sure all passwords are strong and unique.

- Think carefully before connecting devices to the network; it is necessary to change default settings, have strong passwords, and understand embedded security features for each device.
- Enable multi-factor authentication, which involves a second form of authentication required alongside the password; this can be a unique code sent to your mobile device or a retina or fingerprint scan.
- Regularly update the router and connected devices.
- Install a network security solution to detect intrusions or set up one or more guest networks; separate networks on your router to keep computers and smartphones apart from your other devices.

With every connected device posing a threat, consumers will do well to embed security into their expanding smart homes.

Appendix

Methodology

This report was compiled based on a combination of Omdia's continuous research, including market trackers and market forecasts, and primary and secondary research across the relevant topic areas.

Author

Hollie Hennessy
Senior Analyst – IoT Cybersecurity
hollie.hennessy@omdia.com

Mike Sullivan-Trainor
Director – Cybersecurity Consulting
mike.sullivan-trainor@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.